NASPNCLA INSTRUCTION 5510.10D

Subj: NAS PENSACOLA INFORMATION AND PERSONNEL SECURITY MANUAL

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5530.14B
(c) OPNAVINST 3070.1A
(d) SECNAVINST 5212.5C
(e) SECNAVINST 5720.44A
(f) OPNAVINST 5530.15
(g) SECNAVINST 5231.1C
(h) OPNAVINST 5239.1B
(i) NASPNCLAINST 5231.2C
(j) NASPNCLAINST 5500.1D
(k) PL100-235 Computer Security Act of 1987
(l) SECNAVINST 5870.5

1. Purpose. To consolidate NAS Pensacola policies pertaining to information and personnel security, and to implement the procedures and guidance of references (a) through (n).

2. Cancellation. NASPNCLAINST 5510.10C

3. Scope. Policies and procedures set forth herein apply to military and civilian employees of NAS Pensacola, employees of civilian contractors authorized to perform their duties in areas under the jurisdiction of NAS Pensacola, and vendors and visitors authorized entrance to spaces under the authority of NAS Pensacola. Nothing herein shall be construed to nullify directives issued by higher authority. Inquiries for guidance and additional interpretation should be addressed to the NAS Pensacola Security Manager (Code 11000).

4. Action. All NAS Pensacola departments and employees will become familiar with and conform to the policies and procedures set forth in this publication.

5. Forms

a. The following forms referenced in this instruction are available through normal supply channels:

- CNET-GEN 5521/1, Classified Material Access Certification
- OPNAV 5216/10, Correspondence/Material Control
- OPNAV 5511/12, Classified Material Destruction Report
- OPNAV 5520/20, Certificate of Personnel Security Investigation, Clearance, and Access

- OPNAV 5511/30, Classified Container Information
- SF-52, Request for Personnel Action
- SF-86, Questionnaire For National Security Position

- SF-86A, Continuation Sheet for SF 86
- SF-702, Security Container checklist
- SF-703, Top Secret Cover Sheet
- SF-704, Secret Cover Sheet
- SF-705, Confidential Cover Sheet
- SF-312, Classified Information Nondisclosure Agreement

b. The following forms may be obtained from the Administration Department, Code ADAP:

- NASP 5521/10, Classified Material Indoctrination Certification/Proof of U.S. Citizenship
- NASP 5521/17, Security Clearance Medical Questionnaire

J. M. DENKLER

Distribution:
A C
(NASPNCLAINST 5216.1S)

Stocked:
Commanding Officer
NAS Pensacola
190 Radford Blvd
Pensacola, FL 32508-5217

TABLE OF CONTENTS

APPENDICES

CHAPTER 1 - PROGRAM MANAGEMENT

100. Introduction

a. General. The overall Security Program at NAS Pensacola consists of two separate, but related programs:

(1) Information and Personnel Security Program

(2) Physical Security and Loss Prevention Program

b. Purpose. The purpose of this manual is to provide guidelines for administration of the Navy's Information and Personnel Security Program at NAS Pensacola. This manual does not replace and must be used in conjunction with reference (a). Repetition of those parts of reference (a) which do not require additional instruction is avoided in this manual.

c. Updating this Manual. The NAS Pensacola Security Manager has overall responsibility for updating and changing the contents of this manual. All changes, updates, and recommendations for improvement to this manual shall be submitted in writing to the Security Manager, NAS Pensacola Administration Office (Code 11000), Building 624.

101. Command Security Manager (CSM). The CSM will be designated by name and identified to all members of the command on organization charts, telephone listings, and rosters. The CSM shall report to the Commanding Officer on matters of security and is responsible to the Executive Officer for the

administration of the Information and Personnel Security Program. The CSM is the principle advisor and must provide the guidance, coordination, and oversight necessary to ensure the program is being administered effectively. The CSM will be assigned from the Administration Department as a collateral duty and must be a U.S. citizen, officer, or a civilian employee GS-11 or above. The rank requirements are firm and the CSM must have a satisfactory background investigation (BI). The job of CSM should not be passed around to individuals on short-term basis. Duties of the CSM are listed in paragraph 2-8 of reference (a).

102. Security Assistant. The NAS Pensacola Security Assistant will be assigned to the Administration Department to perform administrative and clerical functions pertaining to the Information and Personnel Security Program under the direction of the CSM. The Security Assistant will normally require a Secret clearance. A pitfall in designating an assistant is assigning an individual in a clerical position and making that individual responsible for administering the program. The Security Assistant is not an Assistant Security Manager and, therefore, does not have the authority nor should be ladened with the responsibility for the program management. This is a responsibility of the CSM. Duties of the Security Assistant include the following:

a. Maintains an up-to-date listing of security clearances for NAS Pensacola personnel in a card file and on a desk-top computer.

b. Routes clearance requests for NAS Pensacola.

c. Reviews local personnel records for those persons requesting or requiring a security clearance.

d. Routes classified messages and information within the Administration Department and command.

e. Conducts inspections of classified material containers in NAS Pensacola departments.

f. Initiates security investigations needed for NAS Pensacola personnel requesting or requiring access to classified information.

103. Assistant Security Manager (ASM). The NAS Pensacola Administrative Services Supervisor is designated the ASM as a collateral duty assignment. The ASM has been designated in order to provide a higher degree of authority and continuity to the overall program, and serves as the CSM when circumstances require the undertaking of duties normally under the cognizance of the CSM. The ASM must be designated in writing and be a U.S. citizen, officer, enlisted E-6 or above, or a civilian employee GS-6 or above. A BI is not required unless the individual is authorized to sign the clearance entry on the OPNAV 5520/20.

104. Management Information Systems Security Officer (MISSO). The MISSO is responsible to the CSM for the protection of classified information being processed in the automated system. The NAS Pensacola MISSO is located in the Management Information Systems Office.

105. Special Security Officer (SSO). Naval Air Station Pensacola is not authorized to receive or store Sensitive Compartmented Information (SCI) and, therefore, does not have an SSO. If any SCI material is received with the notation "To be Opened Only by the Special Security Officer," it must be

returned to the sender by Armed Forces Courier Service with the notation that the command does not have an SSO. The CSM is not responsible for handling or controlling SCI.

106. Security Training. The goal of security training is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified material becomes a natural element of every task. Security education must be provided to all personnel, whether they have access to classified information or not.

a. Security Training Responsibilities

(1) Command Security Manager. Has the overall responsibility for security training in the command.

(2) Department Heads/Supervisors. Responsible for identifying the security requirements of their organizational elements, ensuring personnel under their supervision are aware of security requirements for their particular assignments.

b. Departmental Security Training. Due to the size of the command, the Command Security Manager and Security Assistant cannot personally conduct all security training. To complement security training conducted at the Command General Military Training (GMT) sessions, each department will conduct its own specific training tailored to suit its particular needs.

c. Minimum Requirements

(1) Initial Orientation. Each individual requiring access to classified information will be given a security briefing (Appendix B), by their departmental security representative or supervisor prior to being assigned to duties involving classified access. Having an individual certify that they have "read and understand" the provisions of this manual and reference (a) is not adequate orientation. As a minimum, initial orientation will include the following:

(a) The command security organization will be described and the Command Security Manager identified by name.

(b) Make the new member aware of any special security precautions of the command or department.

(c) Review individual security responsibilities; i.e., prohibition against discussing classified information in nonsecure areas or over the telephone, the obligation to report any attempt by an unauthorized person to acquire classified information, or information which could reflect on the trustworthiness of an individual who has access to classified information.

(2) On-the-Job Training (OJT). The phase of training where application of specific security requirements and procedures is learned. Supervisors must ensure this is accomplished. Do not assume that subordinates, especially newly arriving subordinates, know what they are supposed to do.

(3) Refresher Briefings. Will be given at least annually to those individuals who have access to classified information. At this command, annual refresher briefings will be addressed to the entire command at GMT or at department training sessions. The Command GMT Coordinator will assist the Security Manager in scheduling this training.

(4) Debriefings. An individual will be debriefed by the Security Assistant whenever that individual is no longer required or permitted to have access to classified information. Supervisors will ensure their personnel report to the Security Assistant for this purpose.

107. Security Servicing Agreements. As the host command, NAS Pensacola may perform certain functions related to the Information and Personnel Security Program for tenant commands. These services will be covered by a security servicing agreement listing the specific functions performed by the host for the tenant command. A security servicing agreement does not relieve the tenant Commanding Officer from the responsibility for the security of

classified material in that command. All security servicing agreements will be coordinated through the Command Security Manager, Assistant Security Manager, and Security Assistant.

CHAPTER 2 - ACCOUNTING AND CONTROL OF CLASSIFIED MATERIAL

200. Introduction. For the purpose of this instruction, classified material will apply to classified correspondence, messages, publications, documents, information, and equipment used by this command. Classified material must be safeguarded to ensure only personnel appropriately cleared and having a "need to know" are authorized access. This access must be closely monitored by each department.

201. Control and Distribution. All classified material (except messages and communications security material), shall be distributed through and controlled by the NAS Pensacola Security Assistant in the Administration Department. Any classified material received directly by any department or office shall be delivered (unopened) to the Security Assistant for processing. The dissemination of classified information will be limited strictly to those persons who have been cleared for access per the clearance eligibility criteria set forth in Chapter 23 of reference (a) and Chapter 3 of this manual, and whose official duties require knowledge on a "need to know" basis. The Guardmail System will not be used to transmit or distribute classified material. Telecopiers, facsimile equipment, or similar devices using unsecured telephone lines will not be used to transmit classified information.

a. Classified Documents. Upon receipt of classified documents, an OPNAV 5216/10, Correspondence/Material Control Route Sheet, shall be attached to the document and routed by hand to the Security Assistant, Building 624. An illegible signature shall be supplemented with the printed name.

b. Retention, Receipting, or Transmission. The OPNAV 5216/10 shall not be detached from the document except when the document is to be retained. When the document is retained, the original OPNAV 5216/10 must be signed and returned to the Security Assistant. The department retaining the document shall keep a copy of the control form for internal routing and control. Classified material for transmission shall be prepared as directed in Chapter 15 of reference (a).

202. Control of Printing and Reproduction. Because of the numerous reproduction machines available throughout the command, problems associated with reproducing classified material can be enormous. All classified material will be reproduced only by the Naval Computer and Telecommunications Station (NCTS) or the Defense Automated and Printing Service (DAPS). Equipment located elsewhere is not authorized for reproduction of classified material. All reproduction machines will have signs prominently displayed on or near the equipment advising users of the type of material that can be reproduced per Chapter 11 of reference (a).

203. Telephone Transmission. Classified information will not be discussed or "talked around" on the telephone except as authorized on approved secure telephone/communication circuits. Secure communications systems require special operating procedures to place and receive calls. As set forth in C

Chapter 15 of reference (a), it is not necessary to state "this is not a secure line." Unless special equipment is being used, there is no reason to believe a line could be secure. All nonsecure phones at NAS Pensacola will

display a label stating "do not discuss classified information" (DD-2056), as a reminder, stressing telephone security. This form can be obtained through normal supply channels (S/N 10102-LF-002-0506).

204. Hand Carrying Classified Material. Chapter 16 of reference (a) provides guidance for hand carrying classified material. All classified documents and naval messages will be hand carried by designated couriers. Each department will provide a list of designated couriers to the NCTS. The list shall include the level of classified material each courier is authorized to carry and each courier is required to have a courier card. Departments that receive only a small number of classified messages (i.e., one or two classified messages per month) should call the Security Manager (2-2616) or Security Assistant (2-4372) for guidance on designating couriers. As a matter of policy, the number of designated couriers for each department should be limited; i.e., 2-3 individuals per shift. All hand-carried classified material will be covered and guarded to protect against casual observation of the classified information. A sealed envelope will be used and, if the movement requires transportation other than walking, the material will be double wrapped. An SF-704 or SF-705, Cover Sheet, will be used on all classified material transmitted within the command.

205. Control of Visitors, News Media Representatives, and Photography

a. Visitors are allowed unescorted at the National Museum of Naval Aviation, Fort Barrancas, recreational areas, and other areas of historical interest. Unless opened to the public for a special event, no unescorted visitors are allowed on the aircraft flight lines, squadron spaces, maintenance/storage buildings, or NCTS. All news media will be escorted while on board NAS Pensacola with prior arrangements through the Public Affairs Office. Further guidance is provided in Chapter 4 of reference (e), and Chapter 5 of reference (f).

b. Possession of privately owned cameras and taking personal, unofficial photographs of ceremonies, athletic events, personnel, buildings, and grounds (except in areas specifically designated as restricted) are authorized within the command. The facilities of the communications transmitting and receiving locations are specifically designated restricted areas. Violations of the above will result in confiscation of the film. Confiscated film will be forwarded to Base Security with complete addresses and names of the owners, and the name and organization of the person making the confiscation. If feasible, the film may be developed by the Photo Lab and the unclassified portion returned to the owner; otherwise, the film will be destroyed. Artist's sketches or drawings are subject to the same regulations.

206. Disposal of Classified Material. Unnecessary accumulation of classified material increases the possibility of loss, makes accountability and control difficult, poses a fire hazard, necessitates additional security containers, and causes unacceptable delay if emergency destruction becomes necessary. In order to avoid these situations, classified material, including messages, shall be destroyed by the department retaining the material as soon as it is no longer required, or the retention period has otherwise expired per Chapter 17 of reference (d).

All classified material shall be destroyed by an authorized person having appropriate clearance by chemical decomposition, pulping, pulverizing, shredding (mulching), or mutilation sufficient to preclude recognition or reconstruction of the classified information.

a. Classified Material. Prior to destruction, all classified material will be listed on an OPNAV 5511/12, Classified Material Destruction Report (the route sheet will suffice), with the signature of two witnessing officials (one of the witnesses can be the individual destroying the material). One copy of the destruction report will be forwarded to the NAS Pensacola Security Assistant to be retained for a period of 2 years. A record of destruction is not required for Confidential material per Chapter 17 of reference (a). However, the route sheet, OPNAV 5216/10, shall be annotated to reflect destruction and be retained for 2 years.

b. Witnessing Officials. Persons witnessing the destruction of classified material shall have a security clearance at least as high as the category of material being destroyed and shall be thoroughly familiar with the regulations and procedures for safeguarding classified information.

207. Emergency Destruction Plan. In extreme emergencies, such as natural disasters, civil disturbances, or enemy action, emergency destruction of classified material and mail and postal effects held by NAS Pensacola will be per the following procedures. In some situations, destruction of classified material may be avoided by posting a security guard near the classified material container(s):

a. Classified Material. A copy of this emergency destruction plan will be posted in a prominent location near each classified container. In an emergency involving danger of compromising classified material, all classified material will be destroyed per Chapter 17 of reference (a). All departments in receipt of classified material are responsible for conducting emergency destruction when notified by the Commanding Officer. If the Commanding Officer is not available to order the emergency destruction, the Executive Officer, Command Duty Officer, or Administrative Officer is authorized to initiate the specific orders. Departments shall prepare lists which show the locations of classified material, personnel responsible for destruction, and the recommended place and method of destruction.

b. Method for Emergency Destruction. Classified material will be destroyed, insofar as is possible, by whatever means available, but in an expeditious manner.

c. Mail and Postal Effects. If sufficient advanced warning is received, deliver or dispatch mail on hand, suspend mail operations, and transport postal effects and supplies to a safe area.

(1) When insufficient advance warning is received to permit carrying out the above provisions, postal effects should be disposed of in order of priorities as indicated below:

(a) Official registered mail

(b) Directory Service Cards

(c) Other accountable mail

(d) All remaining mail

(e) All other records, equipment, mail sacks, etc.

(2) When destruction of postal effects is appropriate, items will be shredded to unidentifiable pieces.

(3) Classified equipment contained in registered mail and other nonburnable items shall be smashed beyond recognition and scattered, jettisoned, or buried as practicable.

(4) The destruction of postal effects will be witnessed by two officers when possible. If the foregoing is not available, any combination of officer, enlisted, or two other available personnel should be used as witnesses.

(5) When possible prior to destruction, a list of the items destroyed should be attached to the DD 2259, Report of Audit of Postal Accounts. If the list is short, it may be included in the remarks section of the DD 2259.

d. Destruction of Equipment. When necessary to dispose of equipment that still bears a security classification, destruction shall be accomplished by any means that will prevent recognition and/or reconstruction. These provisions do not apply to classified crept equipment. Many items of communications equipment carry special instructions for destruction. All personnel concerned shall refer to the appropriate instructions prior to destroying any communications equipment.

208. Safekeeping and Storage. Anyone who has possession of classified material is responsible for safeguarding it at all times and, particularly, for locking classified material in appropriate security containers. For guidance and assistance for determining stowage requirements, contact the Command Security Manager or Security Assistant (refer to Chapter 14 of reference (a)). The Command Security Manager or Security Assistant will conduct announced and unannounced inspections of security containers belonging to NAS Pensacola departments.

a. Approved Security Filing Containers and Locks

(1) Only filing cabinets that have been approved by the Federal Government as security filing containers will be procured. Select containers from the National Supply Schedule of the General Services Administration (GSA) and follow the procedures outlined in SECNAVINST 10463.1A. Containers used to store classified material shall not be modified. New security filing cabinets shall not be obtained until a physical security survey of existing cabinets and classified records on hand has been completed.

(2) Only three-position combination dial-type padlocks from which the manufacturer's identification numbers have been obliterated may be used. These are available through normal supply channels (Class 5340, miscellaneous hardware).

b. Nonapproved Security Filing Containers and Locks

(1) Nonapproved filing cabinets which are now in use to safeguard classified material should be replaced by GSA-approved security filing cabinets.

(2) Filing cabinets shall not be modified to the lockbar-padlock variety to provide a means to store classified material.

(3) The use of ordinary padlocks to secure containers of classified material is prohibited. Electrically actuated locks (e.g., cipher and magnetic strip card locks) shall not be used to safeguard classified information.

c. Classified Container Information

(1) A custodian will be assigned to each classified container. The custodian's name, home address, and telephone number must be attached inside the locking drawer of the container (refer to Chapter 10 reference (a)). This information, along with specific location and level of classified material stored, must be provided to the NAS Pensacola Security Assistant.

(2) Standard Form 700, Security Container Information, (Part 1), Instructions to Persons Finding Container Open, will be affixed to the inside of the container holding classified material.

(3) All records of combinations of safes and security areas, Secret and below, under cognizance of NAS Pensacola, shall be recorded on Part A of SF-700 and sealed in Part 2, Security Container Information, and delivered to the Security Assistant for safekeeping. All records showing the combination of locks shall be of the same classification as the highest classification of the material in the container. Tenant commands located at NAS Pensacola will be permitted to store safe combinations at the NCTS. Tenant commands will be responsible for maintaining up-to-date combinations and access lists for their combinations.

(4) Combinations to locks and safes should be given only to those whose official duties demand access to the container. The combination to any classified container should be changed whenever the individual knowing the combination no longer requires access or, at a minimum, annually. See paragraph 14-6(5) of reference (a) for additional guidance.

(5) Custodians of classified containers shall verify identification, clearance level, and authorization of personnel before giving access to their safe(s).

d. Care after working hours. Department Heads shall institute a system of security checks at the close of each working day to ensure classified material held by the department is properly protected. Custodians of classified material shall be required to make a security check which will ensure, as a minimum:

(1) All classified material is stowed in the prescribed manner per Chapter 14 of reference (a). Valuables such as money, jewels, precious metals, narcotics, etc., will not be stored in the same container used to safeguard classified material.

(2) Proper accounting is documented for all classified material which must be passed from watch to watch.

(3) The contents of wastebaskets which contain classified material have been properly stowed or destroyed.

(4) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stowed or destroyed. As a matter of routine during the day, such items shall be shredded or disposed immediately after they have served their purpose.

(5) A record of security checks will be maintained and affixed to the container using SF-702, Security Container Check Sheet. The security check will be made and documented whether or not the safe has been opened.

e. Individual custodian responsibility of classified matter. Personnel of this activity shall not remove classified material from the physical confines of this command without the knowledge and approval of the Commanding Officer. Department Heads are delegated authority for this approval. The Command Security Manager must be advised when anyone in a travel status needs to hand carry classified material to or from the command. In such cases, a complete list shall be prepared by the individual removing the material and appropriately filed until the material is returned. In cases involving retirement, release, or discharge of military or civilian personnel having possession of classified material, such material shall be returned to the source from which received. In the event of transfer of military or civilian personnel, classified material held shall be turned over to the successor upon completion of appropriate receipts.

f. Additional Precautions. Department Heads shall ensure all personnel concerned are indoctrinated in the requirements for rotating the dial of all combination locks at least four complete turns inthe same direction when securing safes, files, ccabinets are held firmly in the locked position when secured. Department Heads shall designate individuals to be responsible for the contents of each container of classified material and such records shall be readily available at all times.

209. Classified Meetings. Classified information will not be disclosed at conferences, symposiums, exhibits, conventions, seminars, or other gatherings without first notifying the Command Security Manager prior to any planned classified meeting. The Command Security Manager will ensure the guidelines and policy in Chapter 19 of reference (a) are adhered to.

210. Security Violations. There are two types of security violations. One results in a compromise or possible compromise of classified information and the other is violation of security regulations but no compromise occurs. Chapter 4 of reference (a) discusses in detail the punitive actions, investigation, and reporting of security violations. All security violations shall be investigated thoroughly, even if there is no actual compromise.

a. Reporting. Departments, in cooperation with the NAS Pensacola Security Officer and Security Manager, are responsible for compliance with security regulations and will follow established policy for corrective action to prevent recurrences involving alleged or actual security violations.

(1) Any person discovering unprotected classified information or an unauthorized disclosure of classified information has two immediate responsibilities: first, to attempt to protect the classified information

from further compromise or risk of compromise; and second, to report the circumstances to a responsible official. If you cannot both protect the classified information and report the occurrence, have someone else make the report while you continue to protect the information.

(2) During working hours in the absence of assigned personnel or nonduty hours, the Command Duty Officer (CDO) or Officer of the Day (OOD), telephone 2-2353, will be notified. Security Police will be dispatched as necessary. The security container(s) or classified material shall be guarded until the duty officer or Security Police arrive. An attempt will be made to secure the classified container(s)/material. In all cases, the Security Manager will be notified as well as the custodian of the classified material. After normal working hours, the custodian of a safe found open will be recalled to make a complete inventory.

b. Investigation and Replies

(1) Upon receipt of notification from the Security Manager alleging that a security violation has occurred, the Department Head shall initiate an inquiry to determine: (a) if a security violation actually has occurred; (b) the responsible individual; (c) whether there has been a loss or possible compromise; (d) disciplinary action to be taken; and (e) action contemplated to prevent recurrences. The results of this investigation, including preventive action, will be reported and returned within 15 working days to the Security Manager.

(2) The Security Assistant will keep a record of all security violations and track the investigations and results.

211. Classification Management and Marking

a. Naval Air Station Pensacola does not have original classification authority. Derivative classification and declassification will be accomplished per Chapter 6 of reference (a).

b. All markings of classified material will be per Chapter 9 of reference (a). The Security Assistant and TSCO shall render technical assistance to departments in determining proper special markings of documents.

212. Operations Security (OPSEC) is the process of planning and action associated with operations and other activities to protect essential secrecy. The aim of OPSEC is to neutralize the threat of foreign and terrorist information gathering and synthesis capabilities that support hostile planning and decision making.

a. Anticipatory OPSEC Planning shall be done by Department Heads prior to the start of an operation of any major activity supported by the command. This planning shall identify OPSEC vulnerabilities, possible harmful foreign actions, essential items to keep Secret, and develop OPSEC measures to eliminate OPSEC vulnerabilities. Departments may be required to submit to the Security Manager a memorandum outlining their OPSEC plans.

b. OPSEC Posture Evaluation. Over a period of time, routines may dull the awareness of personnel to the need for OPEC. Also, the OPSEC posture may need to be evaluated if the command's mission is undergoing a change. These situations require an examination of operational procedures and security

practices by each Department Head. This is not necessarily an inspection, but a method to improve command effectiveness.

c. OPSEC Awareness and Training. Ongoing OPSEC awareness and training will be conducted concurrently with the general security training during the initial orientation, OJT, and refresher briefings (See Chapter 1). Each department shall determine if additional OPSEC training should be conducted prior to special events. Since Air Operations and Port Operations Departments are the most operational elements of this command, these departments may desire to concentrate their security training in this area.

CHAPTER 3 - PERSONNEL SECURITY

300. Introduction. Military and civilian employees shall not be granted security clearances until they are actually candidates for access to classified information. Access and clearance will be considered one and the same. If, for example, an individual has the investigative background and is eligible for Secret clearance but needs only Confidential access for performance of normal duties, then that individual will be granted a Confidential clearance. Clearances will not be granted for administrative convenience or for inadvertent or casual access. The common practice of clearing those who may physically require access to a controlled area, regardless of whether such persons need access to classified information, will no longer be continued. Similarly, clearances are sometimes requested to maintain a "stockpile" of cleared employees and, in some cases, persons are nominated for clearances because they were previously cleared and want to maintain such "status." The goal is to maintain the number of individuals with security clearances to the absolute minimum consistent with operational necessity.

301. Security Clearance Control. To more effectively control the number of security clearances, the following steps will be taken:

a. Establish a system of billet control for Secret clearances.

b. Justify the "need to know" for each security clearance requested.

c. Remove from the security clearance process those individuals who require access to classified facilities but not to classified information (casual access).

d. Establish a policy that the continuing need for access to classified information is the condition necessary for requesting a security clearance.

e. Authorize the Security Manager to grant one-time, short-duration access or "temporary access" (up to 2 weeks duration) to classified information to those persons eligible for the higher clearance level to meet unforeseen operational or contractual situations.

302. Granting Security Clearances. Personnel security clearances will be granted on the basis of "need to know." The "need to know" is defined as "the necessity for access to, knowledge of, or possession of classified information in order to carry out official military or other governmental duties." Responsibility for determining whether a person's duties require access and authorization to receive classified information rests upon the one holding the classified information and not upon the prospective recipient. Personnel who require access to classified information shall be appropriately cleared per Chapters 23 and 24 of reference (a) and the specific procedures listed herein. Departments will adhere to these requirements when requesting access to classified material.

a. Initial Clearance. Military personnel requiring access to classified material or information who have not had a previous clearance or have not received a prior NAC or BI as appropriate to the clearance level requested, and civilian personnel requiring a Confidential, Secret, or Top Secret security clearance, shall report to the NAS Pensacola Security Assistant to complete appropriate forms.

b. Department Heads

(1) Department Heads are responsible for determining who in their department requires access and for ensuring the loyalty, reliability, judgment, and trustworthiness of those with access to classified information. Since a goal of this command and the Navy is to keep the number of individuals with security clearances to an absolute minimum, each Department Head is responsible for determining which billets actually require access to classified information. No one has a right to have access to classified information solely because of rank or position. Since it is expensive and time-consuming to conduct Personnel Security Investigations, especially for high level clearances, individuals who already have the proper investigative background to fill billets requiring security clearances should be used. Each Department Head and Special Assistant shall designate a responsible individual as the Department Security Representative and furnish name of the designated individual to the Security Assistant.

(2) Clearance requests shall be submitted to the Security Manager, via the NAS Pensacola Security Assistant. Part I of CNET-GEN 5521/1 (Exhibit 3A), Classified Material Access Certification, shall be completed and forwarded to the NAS Pensacola Security Assistant for military and civilian personnel. A justification memo from the Department Head will be attached to this form with the following information:

(a) Name and Grade of Nominee

(b) Clearance Level Requested

(c) Job Title

(d) Specific reason/justification for clearance level requested

(e) Billet Sequence Code assigned to

Security Assistants shall ensure that U.S. citizenship has been verified as required by paragraph 20-5 of reference (a). An NASP 5521/10 (Exhibit 3B), Classified Material Indoctrination Certification/Proof of U.S. Citizenship, and a completed security indoctrination briefing questionnaire, signed by applicant, will be forwarded to the Security Assistant. All civilian personnel requiring access shall additionally complete NASP 5521/17 (Exhibit 3C), the Security Clearance Medical Questionnaire, and attach to CNET-GEN 5521/1. After first verifying the clearance justification with the Department Security Representative, the Security Assistant will forward the forms to the Security Manager for signature

(3) Department Heads are responsible for notifying the Security Manager when personnel may no longer be suitable for access to classified information. This may be due to NJP, court-martial, demonstrated unreliability, a change of job assignment, excessive indebtedness, substance abuse, etc. See Chapter 22 of reference (a).

c. NAS Pensacola Security Assistant. Upon receipt of the clearance request forms, the Security Assistant will verify the clearance justification and ensure the forms are properly completed. Pull military service records and request a local records check for civilian personnel. A local service record check on the military applicant shall be by the Security Assistant to verify previous National Agency Check (NAC), Entrance National Agency Check (ENTNAC), or Background Investigation (BI) results, if any, and determine whether the record contains any information which might indicate the clearance should not be granted. The Security Assistant will forward all civilian and military access cards to the Medical Officer for medical records check. If there is any derogatory information found in the personnel/medical record checks, the Security Manager and Security Assistant will determine if access is to be granted.

d. Personnel Support Office (PSO). Upon receipt of a list, PSO will provide support to the Security Assistant when the number of records to be pulled and timeliness of action become a consideration.

e. Human Resources Office (HRO). Upon request, HRO will conduct a local personnel records check on the individual to verify previous National Agency Check (NAC), National Agency Check Inquiry (NACI), or Background Investigation (BI) results, if any, and determine whether the record contains any information which might indicate the clearance should not be granted.

f. Medical Officer. Upon receipt of CNET-GEN 5521/1, the Medical Officer shall research the individual's medical record for any information concerning physical or mental illness of a nature which, in his/her opinion, could cause significant defect in the judgment or reliability of the candidate, or reasons which could cause the candidate to act contrary to the best interests of national security. The Medical Officer shall then complete the second endorsement and return it to the NAS Pensacola Security Assistant.

g. Security Manager

(1) Upon receipt of CNET-GEN 5521/1, an evaluation of the clearance justification and clearance level will be made. If the applicant is being assigned to a billet-controlled clearance, an empty billet must exist or the current holder of the billet is expected to be transferred in the near future and the clearance is needed for turnover/training purposes. If the clearance

justification is approved and the local records check is satisfactory, the Security Manager will sign the CNET-GEN 5521/1, Parts I and II, and retain Part I for the NAS Pensacola personnel security clearance files.

(2) The first part of CNET-GEN 5521/1, Part II, will be completed by the Security Manager, indicating the clearance action taken, and returned to the cognizant department. An OPNAV 5520/20, Certificate of Personnel Security Investigation, Clearance, and Access, shall be prepared for military and civilian personnel who are granted requested clearance. The original certificate on military personnel will be forwarded to Personnel Support Activity Detachment (PERSUPPDET) for inclusion in the individual's service record. A copy will be retained by the Security Assistant for inclusion in the security clearance files. The original certificate on civilian personnel will be forwarded to HRO to be filed in the employee's Official Personnel Folder on the right (permanent) side. A copy will be maintained by the Security Assistant.

(3) An SF-312, Classified Information Nondisclosure Agreement, will be signed and witnessed at the time the Security Manager grants clearance and access. The original OPNAV 5520/20 will be annotated in the comments section, "(Date) SF-312 executed."

h. Timely Processing of Clearance Requests. To permit the timely processing of clearance requests, the CNET-GEN 5521/1 shall be returned to the Security Assistant within 2 working days after receipt.

303. Withdrawal/Revocation of Security Clearances

a. Administrative Withdrawal. An individual's security clearance will be administratively lowered or withdrawn if there is no foreseeable need for access to classified information in connection with official duties or contractual obligations. This withdrawal action is taken without prejudice to the individual's future eligibility to access. The NAS Pensacola Security Assistant will annotate on the OPNAV 5520/20, comments section, indicating the action was taken administratively.

b. Denial or Revocation for Causes. Denial or revocation of security clearance for cause is an adverse personnel security determination as described in paragraph 22-5 of reference (a). Adverse action procedures in paragraph 22-6 of reference (a) must be followed exactly.

304. Civilian Security Clearances

a. Civilian Employment. No civilian will be employed, assigned, or retained in any position if such employment, assignment, or retention is not clearly consistent with the interest of national security. Determinations of suitability or eligibility for civilian employment on any basis other than loyalty are not personnel security determinations and, therefore, are not under the purview of this regulation.

b. Position Sensitivity. Each civilian position in this command will be designated as critical-sensitive, noncritical-sensitive, or nonsensitive. The number of designated sensitive positions will be held to the minimum consistent with mission requirements. Since a position may be designated as

sensitive even though no classified material is handled (e.g., guards handling money/financial records etc.), an individual appointed to a sensitive position does not necessarily require a security clearance. However, the individual filling the position must have the proper investigative background for the position; i.e., a critical-sensitive position requires a completed BI and a noncritical-sensitive position requires a completed NACI. Department Heads will determine which positions should be designated as critical-sensitive, noncritical-sensitive, or nonsensitive by following the criteria in paragraph 20-6 of reference (a). When individual position action is initiated, the SF-52, Request for Personnel Action, will include the security requirements.

305. Continuous Evaluation for Eligibility. Department Heads and supervisors are responsible for the continuous evaluation of their personnel and must be alert for behavior indicating unexplained affluence, financial instability, or alcohol or drug abuse. Such behavior must be brought to the attention of the Security Manager.

306. Foreign Travel Briefings. Any individual who has had access to classified information who plans to travel to or through a communist-controlled country or to attend a meeting in the United States or elsewhere in which representatives of communist-controlled countries are expected to participate must be given a defensive briefings. This briefing will be given by a Naval Investigative Service (NIS) agent. Upon return from travel, the individual will be debriefed by an NIS agent. Each Department Head must make sure personnel know this is a required briefing and they are responsible for advising the Security Manager when a situation requiring a "foreign travel" brief arises. The Personnel Support Officer will ensure “foreign travel” leave papers are annotated by the Security Manger or Security Assistant indicating completion of the defensive briefing.

307. Debriefing. A debriefing will be conducted by the Security Assistant for personnel who have had access to classified information under the following circumstances:

a. Prior to termination of active military service or civilian employment, or temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.

b. At the conclusion of the access period, when a limited access authorization has been granted.

c. When a security clearance is revoked for cause.

d. When a security clearance is administratively withdrawn.

At the conclusion of the debriefing, the employee will be required to read the provisions of the Espionage Act and other criminal statues in Appendix F, OPNAVINST 5510.1, and read the Security Termination Statement (OPNAV 5511/14) and sign it. The witness to the signature then signs the Security Termination statement. A debriefing will be given when someone is being transferred from one command to another but a Security Termination Statement is not required.

APPENDIX A
ORIENTATION BRIEFING FOR ALL PERSONNEL
REPORTING ON BOARD NAVAL AIR STATION PENSACOLA, FLORIDA

1. NAS Pensacola Information and Personnel Security Program. An effective program exists within this command to safeguard against compromise of classified material and information. You are part of this program. During your stay at Naval Air Station Pensacola, you may be required to participate in lectures, films, and other security awareness training. The goal of security training is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified material becomes a natural element in every task. Periodic refresher briefings are given for personnel who have been granted access. Attendance is mandatory.

2. Security Manager. The Administrative Officer, telephone 452-2616, is designated the Security Manager for NAS Pensacola and is available to provide assistance upon request.

3. Personnel Security Clearances. Not every individual has access to classified material. Clearance and access will be granted depending on the requirements of the job. However, all personnel having knowledge of classified material or information are responsible for maintaining security thereof, no matter how that information was obtained.

4. Telephone Transmission. Classified information will not be discussed or "talked around" on the telephone except as authorized on approved secure telephone or communications circuits. The statement "this is not a secure line" is not necessary because unless the special equipment is being used, there is no reason to believe a line could be secure.

5. Foreign Travel. If you have a clearance or access and are contemplating foreign travel, either in a leave or duty status, you are required to contact the Security Manager prior to your travel for a briefing.

6. Violations. If you suspect a security violation, contact the Security Manager immediately (452-2616). Any person discovering unprotected classified information has two immediate responsibilities: first, to attempt to protect the classified information from further compromise or risk of compromise; and second, to report the circumstances to a responsible official. During nonduty hours or during working hours in the absence of assigned personnel, the Command Duty Officer (CDO) or Officer of the Day (OOD), telephone 2-2353, will be notified.

7. I, _____, acknowledge that I have read and understand the above briefing_____ (date).

RETURN TO SECURITY ASSISTANT, NAS ADMINISTRATION, AFTER ORIENTATION AND SIGNATURE.

APPENDIX B
SECURITY INDOCTRINATION BRIEFING
TO BE READ BY EVERYONE BEING GRANTED A SECURITY CLEARANCE AT NAS PENSACOLA
ATTACHED QUESTIONNAIRE WILL THEN BE COMPLETED

1. Commanding Officers are directly responsible for safeguarding all classified information within their commands and for assuring classified material not in actual use of appropriately cleared personnel or under their direct personal observation is stored in the manner prescribed in OPNAVINST 5510.1H, Navy's Information Security Manual.

2. The Administrative Officer is designated the Security Manager for NAS Pensacola and shall assist the Commanding Officer in fulfilling his responsibilities for the security of classified information. The Security Assistant, Administration Department, will serve as the principal assistant to the Security Manager in the development and execution of the station's classified material security program.

3. Department Heads are responsible for the security of classified material within their respective departments and shall designate an individual as a departmental security representative and furnish the name of the individual to the Security Assistant.

4. Every individual in the Department of the Navy who acquires access to classified information is responsible for protecting that information per OPNAVINST 5510.1H. Clearance for access to classified matter is considered extremely important. All personnel having knowledge of classified material are responsible for maintaining security thereof, no matter how that information was obtained.

5. The determination that information requires protection is called classification. Classified information has to be identified/marked with a classification. The classifications, in order of the highest security level to the lowest, are TOP SECRET, SECRET, and CONFIDENTIAL. Each classification requires specified protective measures. The loss of any classified material will result in damage to the national security.

6. Classified information may only be given to individuals who have been authorized access to it. Just as classified material is assigned levels of classification, there are different levels of personnel security clearances. Individuals are cleared for access to the level of information they will require in their job. For example, a person whose job requires access to Secret material will be given a Secret clearance and may have access to Secret and Confidential information, but not Top Secret. However, just because you hold a Secret clearance does not mean you have access to all Secret information. You must also have a "need to know;" that is, besides having the proper clearance, your official duties must require that you have the information.

7. Safeguarding requirements permit classified information to be used or stored only where and when it can be properly protected. This means there are many things you may not do with classified information. YOU MAY NOT:

a. Leave classified information unprotected - it must either be properly stored or in the custody of a cleared person.

b. Read or discuss classified information in an unsecured area -- classified information may be used only where uncleared persons or persons without a need to know will neither see nor hear it.

c. Remove classified information from the command -- except in approved situations and with specific permission of the Commanding Officer or other designated official.

d. Reproduce classified information -- except as approved by a designated official.

e. Give classified information to a visitor without first verifying the visitor's identification, clearance, and need to know.

f. Discuss classified information over the telephone.

g. Send classified information out of the command by other than approved methods.

h. Dispose of classified information by other than approved methods and with the required records.

i. Store security container combinations in insecure places; e.g., wallets, under desk blotters, etc.

j. Take classified information with you when you leave this employment -- classified information is official information, not personal property.

8. You are responsible for ensuring any classified material in your possession is safeguarded. A security representative has been designated within each department to advise you of specific procedures within your office. The following are our command requirements:

a. During work hours, classified material on desks and in routing baskets should be placed face down when not in use.

b. If leaving for lunch or a coffee break, classified material must either be locked up or under continuous observation by a cleared individual.

c. Do not ask a messenger to pick up or deliver classified matter without verifying that person's clearance.

d. Upon securing for the day, all desks are to cleared of classified material and the material locked up.

e. Locked desk drawers or briefcases may not be used, even temporarily, to safeguard classified material.

f. Tumbler locks on safes are to be spun at least four times and drawer handles pulled to ensure the container is locked. The SF-702, Security Container Check Sheet, on top of the container should then be initialed and witnessed.

9. All personnel answering the telephone in spaces where classified or sensitive information is processed must be aware of conversations which discuss or touch on classified information -- immediately terminate conversation for a more secure means of communications (AUTOSEVOCOM, SECURE TTY, DATA CIRCUITS). Personnel should not discuss or transmit classified

information over the telephone or in such manner as to be intercepted by unauthorized persons.

10. Sometimes when the rules are not followed or somebody makes a mistake, a situation will occur in which classified information may be compromised. Any person discovering unprotected classified information has two immediate responsibilities: First, to attempt to protect the classified information from compromise or risk of compromise; and second, to report the circumstances to a responsible official. If you cannot both protect the classified information and report the occurrence, have someone else make the report while you continue to protect the information. If you are ever approached by someone and asked to make an unauthorized disclosure of classified information, don't try to handle the situation yourself -- Report it immediately to your Security Manager (452-2616) or supervisor. REMEMBER, SAFEGUARDING CLASSIFIED INFORMATION IS A TEAM EFFORT. IF YOU NEED HELP --- SEEK IT.

11. Any individual who has had access to classified information and plans to travel to or through a communist-controlled country or to attend a meeting in the United States or elsewhere in which representatives of communist-controlled countries are expected to participate must be given a defensive briefing. This briefing will be given by a Naval Investigative Service (NIS) agent. When the individual returns, they will be debriefed by an NIS agent.

12. Please answer the questions on the attached sheets and return to your department security representative for discussion. The department security representative will then forward the completed questionnaire to the NAS Pensacola Security Assistant.

APPENDIX C
SECURITY QUESTIONNAIRE

The following questions are designed to find out if you understand some basic facts about the Navy's Information Security Program. After you have answered all questions, the correct answers will be provided and discussed.

1. The security classification categories, in order from highest to lowest, are:

a. SECRET, CONFIDENTIAL, RESTRICTED

b. TOP SECRET, SECRET, CONFIDENTIAL

c. SECRET, CONFIDENTIAL, FOR OFFICIAL USE ONLY.

d. TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED

2. No one has a right to have access to classified information solely because of rank or position. _____ True _____ False

3. Classified information may be revealed to which of the following?

a. Any military person.

b. Any person with an appropriate clearance.

c. Any person whose job requires it.

d. Any person with an appropriate clearance and a need to know.

4. A person with a Secret clearance may be given access to:

a. Secret and Confidential information.

b. Only Secret information.

c. Secret and Top Secret information.

d. Top Secret, Secret, and Confidential information.

5. It is not permissible to use the Guardmail System to transmit or distribute classified information. _____ True _____ False

6. Which of the following statements about information security is true?

a. Classified information may be discussed over the telephone on local calls.

b. Classified information which you originate is your personal property and may be taken with you when you leave Navy employment.

c. Classified information may only be reproduced when approved by an designated official and only on authorized reproduction equipment.

d. Classified material may be left unprotected for short periods of time during the working day.

7. Which of the following are true statements about disposal of classified documents?

a. Confidential material may be disposed of by any method normally used to dispose of waste material.

b. Classified documents may never be destroyed.

c. Classified material must be disposed of by methods approved for destruction of classified material and with necessary records.

d. Downgrading the document removes any restrictions on disposal.

8. Classified information may be disclosed to a visitor after:

a. The visitor's identification has been verified.

b. The visitor's clearance has been verified.

c. The visitor's need to know has been verified.

d. All of the above.

9. If you discover unprotected classified information or an unauthorized disclosure of classified information, you should:

a. Immediately notify a responsible official.

b. Protect the classified information from further compromise or risk of compromise.

c. Do nothing. It is not your responsibility.

d. Do both a and b.

10. The Security Manager is the command's advisor on matters pertaining to the Information Security Program.

_____ True _____False

APPENDIX D
USE OF PERSONALLY OWNED COMPUTER SYSTEMS IN NAS PENSACOLA ORGANIZATION WORKSPACES
POLICY STATEMENT

1. Policy. The policy of Naval Air Station Pensacola is to permit the use of personally owned computers in organizational workspaces, for the purpose of accomplishing job-related work, only with the prior written approval of the Commanding Officer and subject to the conditions and limitations provided herein.

2. Conditions and Limitations. Applicability of these provisions extends to all hardware, software, components, and peripheral devices which comprise the personally owned computer system.

a. Use of a personally owned computer is for the personal convenience of the requester and not at the direction of a manager or supervisor.

b. Government liability for loss, damage, or theft of a personally owned computer is limited (under qualifying conditions) to $200 per claim. Liability insurance coverage on a personally owned computer is the responsibility of the owner; requests for approval must certify such proof of insurance.

c. Characteristics of files and records produced on personally owned computers will be predicated upon the data technical standards of the command, and not upon those of the personally owned computer. Specifically, if files and records produced on a personally owned computer may be required for use on government equipment, the personally owned equipment must meet all standards for compatibility with such government equipment.

d. Files and records created, used, or stored on personally owned computers are limited to "For Official Use Only" and become the property of the United States Government.

e. Managers and supervisors will assume the same responsibilities for use of personally owned computers as for government equipment.

- Files and records will remain accessible to the Government, whether or not the owner/requester is present or the personally owned computer is on board, removed, or becomes inoperable;

- Equipment, files, and records will be afforded the degree of protection necessary to ensure both physical security and data integrity.

f. Managers and supervisors will ensure personal and Government property ownership and accountability are not mixed. Personally owned hardware and software will be clearly labeled; Government equipment will be identified. as required by established ADP Security and Plant/Minor Property accounting procedures.

g. Personnel, equipment, and/or material requirements are based on the needs of the organization, without regard to the number of personally owned computers present in the workspace.

3. Procedures

a. Memorandum requests for use of personally owned computers shall reference this Appendix, and be submitted from the owner/requester to the Commanding Officer, via appropriate chain command and the ADP Security Officer (Code 00S00), Building 624.

b. At a minimum, requests shall contain the following information:

- Listing of system hardware (nomenclature, make, model, serial number)
- Listing of system software (product name, version, serial number)

- Description of what the system will be used for (tasks/work to be performed)

- Certification that system hardware and software are adequately insured by private insurance of the requester.

APPENDIX E
STANDARD OPERATING PROCEDURES
FOR
NAVAL AIR STATION PENSACOLA
AUTOMATED INFORMATION SYSTEMS

1. Purpose. The purpose of this document is to establish standard operating procedures (SOP) for operation of automated information systems (AIS) to comply with requirements of the Department of the Navy (DON) Automatic Data Processing (ADP) Security Program and Naval Air Station Pensacola ADP Security Program.

2. Scope. The SOP will be used to ensure all authorized users are properly instructed of their responsibility in the operation, maintenance, and security of the equipment located within NAS Pensacola departments and staff offices.

3. Standard Operating Procedures

a. System Operating Procedures. Start-up, operation, and shutdown of the system shall be per equipment operating procedures provided by the vendor or by government regulations.

b. Level of Data Processed. No classified information will be processed or stored on the system. Level II data will be safeguarded in the same manner as 'FOR OFFICIAL USE ONLY" data. The system will be used for official business only.

c. Malicious Code. Special care shall be taken to reduce the risk of introduction of malicious codes such as logic bombs, Trojan horses, trapdoors, and viruses into computer systems. Terminal Area Security Officers (TASO's) will ensure only authorized software is permitted for use on the system. Periodic inspections will be performed to ensure compliance and enforcement of system security.

d. Access Control. Only persons authorized by the department, division, or branch head shall operate the system. Authorization for nongovernment employees must be in writing. The Management Information System Security Officer (MISSO) will provide authorized personnel access lists to the Information System Security Officer (ISSO) and passwords will be issued as required.

e. Individual Accountability. Access to AIS's, networks, and other computer resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

f. Media Protection. When system is unattended for extended periods and during nonworking hours, all Level II output, software, and data files on removable media (e.g, printed output, diskettes, tapes, disks, cassettes, etc.) will be labeled appropriately and secured. If Level II data is stored on a hard disk, the system must be shut down and physically secured in a locked office during nonworking hours.

g. Data Protection. During periods of operation, data files will be protected and restricted to authorized users on a need-to-know basis. Automated Information Systems must not be left unmonitored while Level II data is on the screen.

h. Physical Security. All reasonable precautions will be taken to prevent loss or damage to the systems and its components.

i. Backup Schedule. A routine schedule for daily and weekly backups on tapes or disks will be enforced by the department, division, or branch head to ensure protection against loss of data.

j. Physical Care of Automated Systems. Keep work area around system free of dust that could be drawn into the computer. No smoking will be allowed around automated systems. When equipment is not in use, use plastic covers, if available, to protect against damage due to fire, smoke, water, or other natural disasters.

APPENDIX F
INFORMATION SYSTEMS CONTINGENCY PLAN
FOR
NAS PENSACOLA
DEPARTMENTS AND STAFF OFFICES

1. The Management Information Systems (MIS) Office has established an informal Contingency Plan with all Naval Air Station Pensacola departments and staff offices having a microcomputer, word processor, or terminal. These automated information systems (AIS's) are primarily used for word processing, data base management, and spreadsheet application programs.

2. If an AIS becomes inoperable and loss of processing capability poses a potential problem or critical situation for the department/special assistant, notify the MIS Office, 2-2034. The MIS Office will make appropriate arrangements to replace the system or provide access to another system. If required, the MISO will provide recovery operations for lost data files.

3. Daily and weekly backup copies of data files will be accomplished by the Terminal Area Security Officer (TASO) or a designated operator of each stand-alone system. A recommended schedule would be to backup daily only the files that have been changed that day and backup the entire system every week. Keep 2 weeks worth of backups, the current week and the past week, and rotate the use of diskettes or tapes. Refer to your DOS manual for the exact syntax of the backup command. The MISO provides backup operations for the Executive Information Systems.

4. Destructive weather security procedures to prevent damage to AIS during hurricane preparation, severe storms, tornado's, etc., are as follows:

a. Ensure hurricane gear (e.g., tape, rope, plastic sheets) is readily available. Upon setting of Condition III (within 48 hours), secure all AIS equipment. When Condition II (within 24 hours) has been set, place AIS equipment and peripherals, including backup tapes and/or diskettes, in a high, well-protected area away from water damage. Cover all AIS equipment and furniture with plastic covering and secure with line or tape.

b. In the event of a severe thunderstorm or tornado warning, shutdown system in accordance with the system Standard Operating Procedures.

APPENDIX G
NAS PENSACOLA FLORIDA
EMERGENCY ACTION PLAN

1. The following procedures will be adhered to when required by holders of classified material at Naval Air Station Pensacola.

a. UNSECURED CLASSIFIED CONTAINER. In the event a classified container is found unsecured (open), the person discovering the discrepancy will take the following action:

(1) Attempt to notify the custodian indicated on the front of the container.

(2) If unable to notify the custodian, notify the NAS Pensacola Officer of the Day (OOD) or the NAS Pensacola Command Duty Officer (CDO) at extension 2-2353 or 2-2354.

(3) Remain at the location of the unsecured container until relieved by the custodian, the OOD, or the CDO.

(4) Whomever secures the container is responsible for notifying the Command Security Manager (CSM) at extension 2-2616 during duty hours of the next working day of the circumstances surrounding the discrepancy.

(5) The custodian is required to take inventory or the container contents upon their arrival, and notify the CMS, in writing, of the results of the inventory.

(6) Based upon all information received, the CSM may or may not implement requirements for a "Possible Compromise" JAGMAN investigation.

b. EMERGENCY DESTRUCTION. Upon declaration by the Commanding Officer or his designated representative to implement emergency destruction, the following procedures are required:

(1) Take necessary action to destroy material in the following sequence:

PRIORITY ONE - Top Secret Material

PRIORITY TWO - Secret Material

PRIORITY THREE - Confidential Material

(2) Method of destruction will be by the most expeditious method available. In the case of classified equipment, destruction shall be by whatever means available to render the equipment to such a point that it can not be reconstructed to a recognizable status.

2. This Emergency Action Plan (EAP) is to be posted in the immediate vicinity of containers utilized for classified material.